Gemeente Amsterdam

Werkinstructie afhandeling datalekmeldingen

CONCEPT

Vakgroep Digitale Rechten, Ethiek en Privacy
Digitalisering, Innovatie en Informatie (DII)
Digitale Strategie en Informatie (DSI)
Versie 0.5 – 20 december 2024

Inhoudsopgave

1. Inleiding 3
1.1 Doel & doelgroep 3
1.2 Datalek: inbreuk op persoonsgegevens en betrokkenen 4
1.3 Rol en taakverdeling (governance) datalekkenprocedure 4
1.4 Benodigde toegang tot mailbox en TOPdesk 4

2. Stappenplan datalekkenprocedure 5
2.1 Maakt melding 6
2.2 Analyseert datalek 6
2.3 TOPdesk melding invullen 7
2.4 Vraag extra informatie 7
2.5 Geeft informatie 7
2.6 Maak voorlopige melding bij AP 7
2.7 Vraag FG om advies 8
2.8 Adviseert over AP en informeren betrokkenen 8
2.9 Trek AP melding in 9
2.10 Maak AP melding definitief 9
2.11 Maatregelen adviseren 9
2.12 Adviseert directie dringend betrokkenen te informeren, evt. maatregelen die betrokkenen zelf kunnen nemen 9
2.13 Informeert betrokkenen 10
2.14 Treft geadviseerde maatregelen 10
2.15 Melding volledig maken, afmelden in TOPdesk 10
2.16 Ontvangt afmelding 10
2.17 Ontvangt afmelding 10

3. Bijlagen 11

Bijlage 1: Handleiding TOPdesk 12
Inhoudsopgave 12
1. Startpagina, meldingen en zoeken 13
2. Nieuwe melding aanmaken (tab: Algemeen) 14
3. Beveiligingsincident invullen 16
3.1 Beveiligingsincident registreren 16
3.2 Beveiligingsincident als datalek samenvatten 17
4. Communiceren met de melder 19
5. TOPdesk standaardteksten instellen (eenmalig) en gebruiken 20
5.1 Standaardtekst toevoegen 20
5.2 Standaardtekst verdeling 21
5.3 De negen standaardteksten 21
5.3.1 – Standaardtekst 1 21
5.3.3 – Standaardtekst 3 22
5.3.4 – Standaardtekst 4 23
5.3.5 – Standaardtekst 5 23
5.3.6 – Standaardtekst 6 24

5.3.7 – Standaardtekst 7.....25
5.3.8 – Standaardtekst 8.....25
5.3.9 – Standaardtekst 9.....25

Bijlage 2: Standaardbrief t.b.v het informeren van betrokkenen..... 28

Bijlage 3: Analyse van veelvoorkomende datalekken (volgt in 2025)..... 34

1. Inleiding

De vakgroep Digitale Rechten, Ethiek en Privacy is eigenaar van het meldpunt datalekken, bereikbaar via 5.1, 2, i @amsterdam.nl. Dit meldpunt is de centrale plek waar datalekken - waarvoor de Gemeente Amsterdam (mede)-verwerkingsverantwoordelijke is – worden gemeld. Na melding worden deze datalekken door een Privacy Officer behandeld. Omdat tijdens weekdagen meerdere Privacy Officers deze meldingen bekijken en in behandeling nemen, is het essentieel om de werkwijze procedureel vast te leggen. Deze procedure beschrijft niet wanneer en hoe een datalekmelding moet worden gedaan, maar hoe de afhandeling plaatsvindt.

Dit eerste hoofdstuk beschrijft:

- het doel en de doelgroep van de procedure
- een korte definitie van datalekken
- de rolverdeling binnen de procedure
- benodigde systemen voor elke Privacy Officer

Hoofdstuk 2 gaat dieper in op de behandeling van datalekken door de Privacy Officer. In hoofdstuk 3 worden tot slot relevante bijlagen vermeld t.b.v. de uitvoering van de procedure. Dit zijn handleiding TOPdesk, de brief t.b.v. het informeren van betrokkenen en, in een latere versie, een analyse van veelvoorkomende datalekken.

1.1 Doel & doelgroep

Deze datalekkenprocedure beschrijft de behandeling van datalekken binnen de Gemeente Amsterdam. De datalekkenprocedure helpt ervoor om te zorgen dat Privacy Officers op een eenduidige wijze datalekken behandelen.

De doelgroep van het document is primair de Privacy Officer die piketdiensten draait. Deze diensten vinden plaats gedurende werkdagen (8:30 – 17:30). Via de vakgroepmanager of teamleider Privacy wordt de Privacy Officer ingedeeld in een dienst. De piketdiensten vinden plaats tijdens vakantie- en feestdagen. Naast de Privacy Officer vervult ook de Functionaris Gegevensbescherming (hierna; FG) een belangrijke rol in de procedure.

Behandelende Privacy Officers worden verondersteld voldoende kennis te hebben m.b.t. de relevante artikelen en beginselen uit de Algemene Verordening Gegevensbescherming (AVG) en de Wet Politiegegevens (Wpg). Met deze kennis zijn ze in staat om de procedure zelfstandig te volgen. Uiteraard wordt overleggen met collega's binnen de piketdiensten – of met de FG – waar nodig aanbevolen.

1.2 Datalek: inbreuk op persoonsgegevens en betrokkenen

Binnen de Gemeente Amsterdam zijn twee definities relevant. Allereerst AVG artikel 4 (12), welke een datalek als volgt beschrijft:

"inbreuk in verband met persoonsgegeven": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens

De definitie binnen de Wpg is overeenkomstig – maar spreekt expliciet over politiegegevens.

Een inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of toegang tot politiegegevens.

1.3 Rol en taakverdeling (governance) datalekkenprocedure

Er zijn vier actoren binnen de datalekkenprocedure. Dat zijn:

- **Melder datalek.** Meldt het datalek en verstrekt informatie over het datalek.
- **Privacy Officer (PO).** Handelt een datalek af (niet; voorkomt herhaling of implementeert maatregelen).
- **FG.** Geeft advies over de risico-inschatting van het datalek.
- **Directie.** Is verantwoordelijk voor het werkproces en evt. geadviseerde maatregelen – om bijvoorbeeld herhaling van het lek te voorkomen. Wordt soms geacht betrokkenen te informeren.

NB: De Autoriteit Persoonsgegevens (hierna; AP) is hier bewust niet meegenomen, ondanks hun mogelijke rol in het proces.

De Privacy Officer werkt tijdens de afhandeling van een datalek in de applicatie TOPdesk. Dit is een gemeentebreed servicemanagementsysteem waarbinnen het datalekkenregister (AVG, Wpg) is opgeslagen. Het is verplicht dat voor elk datalek goede verslaglegging plaatsvindt. Zo komt niet alleen de aanleiding en feitelijkheid van het datalek in beeld, maar ook geadviseerde maatregelen en andere relevante informatie, zoals informatie over een melding bij de AP. Persoonsgegevens Operationele informatie over hoe TOPdesk moet worden gebruikt, lees je in **Bijlage 1: Handleiding TOPdesk.**

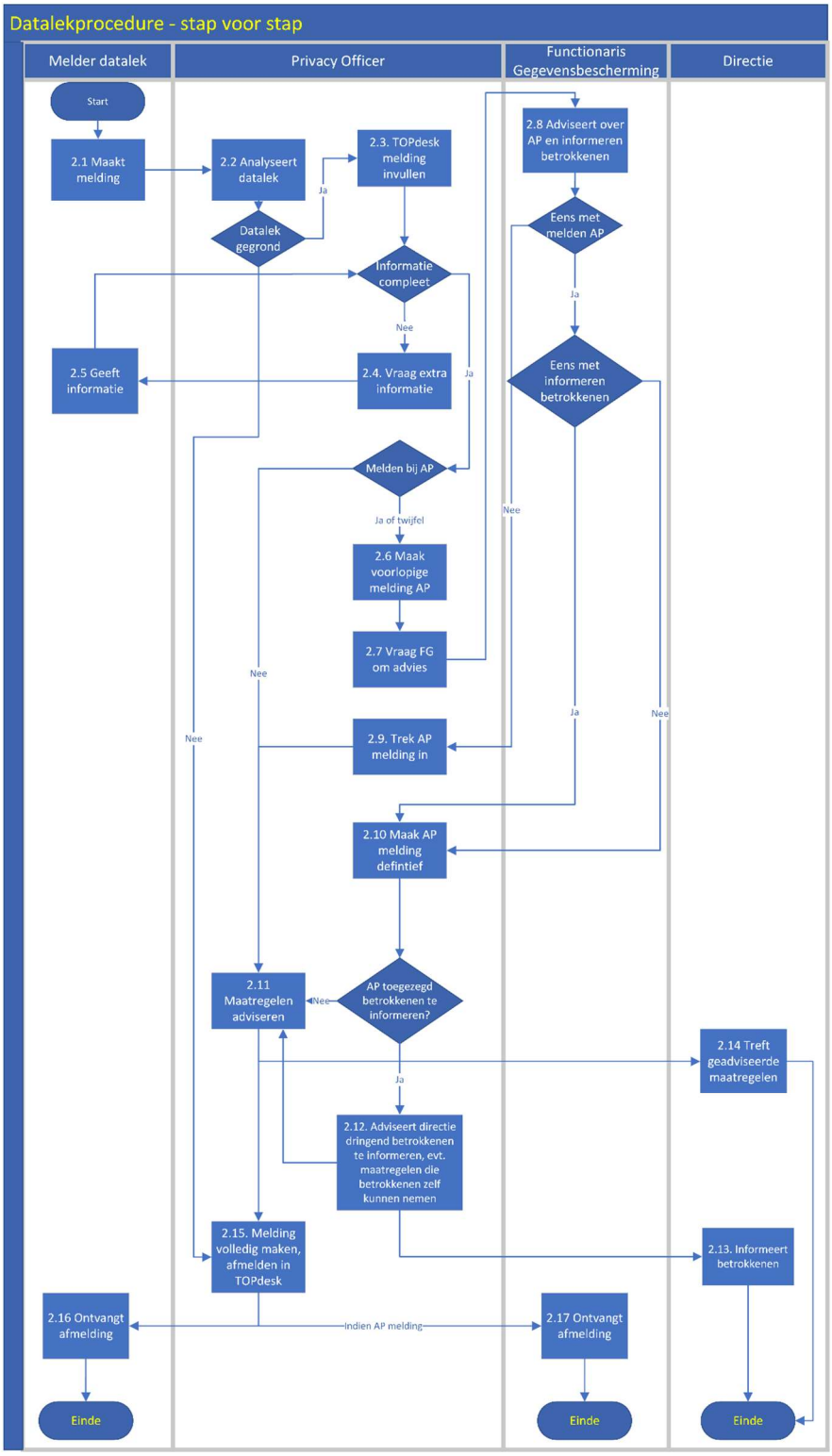
Soms betreft een datalek politiegegevens. Dit is bijvoorbeeld te herkennen wanneer een melder aangeeft dat de gegevens verzameld zijn door een boa – of zijn verkregen van de politie. Wanneer dit datalek een mogelijk hoog risico oplevert voor betrokkenen of de opsporing, is het altijd goed om de Privacy Officer Wpg van de Gemeente Amsterdam te betrekken. Binnen de Wpg zijn er bijvoorbeeld meer uitzonderingsgronden om betrokkenen niet te informeren.

1.4 Benodigde toegang tot mailbox en TOPdesk

De Privacy Officer heeft toegang nodig tot de mailbox 5.1, 2, i @amsterdam.nl en toegang tot TOPdesk, de servicemanagement omgeving van de Gemeente Amsterdam. Beide kunnen worden aangevraagd bij je leidinggevende via adres 5.1, 2, i @amsterdam.nl.

2. Stappenplan datalekkenprocedure

Dit tweede hoofdstuk beschrijft stap voor stap de procedure die wordt gevolgd wanneer er (mogelijk) sprake is van een datalek. In afbeelding 1 is het stappenplan afgebeeld. Elke stap is genummerd – deze nummering komt overeen met de hoofdstukken.



Afbeelding 1 – proces datalekkenprocedure

2.1 Maakt melding

De melder van het datalek meldt dit bij de Gemeente Amsterdam. Dit kan via TOPdesk (vindbaar via het intranet) of rechtstreeks via 5.1, 2, i @amsterdam.nl (voor externen). Het TOPdesk formulier dwingt de collega om het datalek uitvoerig te beschrijven en is de vaste werkwijze voor collega's.

Van meldingen die via TOPdesk worden gedaan worden ook e-mails richting 5.1, 2, i @amsterdam.nl gestuurd. Toch is het goed om tijdens een piketdienst ook TOPdesk in de gaten te houden – soms worden meldingen door collega's doorgezet die bijvoorbeeld een beveiligingsincident daar markeren als (mogelijk) datalek.

Externe partners van de Gemeente Amsterdam – bijvoorbeeld verwerkers met verwerkersovereenkomsten – zijn in regel op de hoogte van het e-mailadres van het meldpunt datalekken.

2.2 Analyseert datalek

Niet in alle gevallen is een binnengekomen datalek ook echt een datalek. Daarom moet de Privacy Officer allereerst beoordelen of er sprake is van een datalek. Als dit niet het geval is, mag de melding worden afgesloten in TOPdesk. Let erop dat de melding dan niet is geregistreerd als *gegrond* – zie ook **Bijlage 1: Handleiding TOPdesk.**

In alle andere gevallen is het belangrijk om het datalek volledig te omschrijven. Gebruik hiervoor de informatie die is verstrekt door de betrokkene en wees kritisch. Soms zijn de meldformulieren niet volledig ingevuld, of moet er tussen de regels door gelezen worden om het volledige lek te begrijpen.

Tip: Vat kort samen wat het verhaal omtrent het datalek is om na te gaan of je alle relevante informatie hebt.

1. Wat is er wanneer gebeurd
2. Wat is de oorzaak van het datalek
3. Welke gegevens zijn gelekt en hoe gevoelig zijn deze
4. Wie zijn de betrokkenen en hoeveel betrokkenen zijn er
5. Welke maatregelen zijn er tot heden getroffen om dit datalek te stoppen
6. Wat zouden de gevolgen kunnen zijn voor de betrokkenen (bijvoorbeeld risico op identiteitsfraude, discriminatie, reputatieschade, financiële schade)
7. Is een melding aan de AP noodzakelijk?
8. Is een melding aan betrokkenen noodzakelijk?

Punten 1 t/m 5 gaan over feitelijke informatie. Punten 6 t/m 8 vragen je een inschatting te maken over hoe ernstig het datalek is.

Bekijk ook de website van de autoriteit persoonsgegevens en bestudeer waar nodig de Guidelines 01/2021 on Examples regarding Personal Data Breach Notification

2.3 TOPdesk melding invullen

Zorg ervoor dat conform **Bijlage 1: Handleiding TOPdesk** het datalek wordt vastgelegd en de relevante velden worden ingevuld.

2.4 Vraag extra informatie

Is de melding niet duidelijk? Heb je meer informatie nodig? Of begrijp je het relevante werkproces niet? Dan is het aanbevolen om telefonisch contact op te nemen met de melder – en anders per e-mail. Houd hierbij rekening met een eventuele meldplicht bij de AP, uiterlijk 72 uur na *kennisname*. Kennisname betekent hier niet kennisname door de Privacy Officer, maar kennisname door de organisatie, het moment dat bekend werd dat een situatie een datalek was.

Tip: via zoek een collega vind je vaak contactgegevens van melders – en vaak een leidinggevende.

2.5 Geeft informatie

De melder geeft de benodigde informatie aan de Privacy Officer.

2.6 Maak voorlopige melding bij AP

De Privacy Officer maakt een risico-inschatting voor betrokkenen, zodra alle informatie voorhanden is. Het is belangrijk dat - waar mogelijk - er maatregelen worden geadviseerd aan de melder en evt. diens directie. Zo voorkom je herhaling van het datalek– of wordt de impact op betrokkenen verkleind. Dit is belangrijk, ook wanneer er geen melding wordt gedaan bij de AP. Daarom wordt bij elk datalek verwezen naar *2.11 Maatregelen adviseren.* In veel gevallen is het niet waarschijnlijk dat een datalek een hoog risico oplevert voor de betrokkenen. In zo'n geval hoef je geen melding te doen bij de AP. Maar soms is dat wel nodig.

Is er een hoog risico denkbaar voor betrokkenen of twijfel je? Je kunt dan overleggen met de FG. Is de FG niet bereikbaar? Maak dan gelijk een melding bij de autoriteit persoonsgegevens. Het is essentieel dat binnen 72 uur na kennisname melding bij de autoriteit persoonsgegevens wordt gedaan. Let op; we maken de melding in eerste instantie **altijd** voorlopig.

Via **https://datalekken.autoriteitpersoonsgegevens.nl/** kan een (voorlopige) datalekmelding worden gedaan. Of maak je (voorlopige) meldingen definitief. Aan het begin moet de volgende informatie worden ingevuld:

- Registratienummer van de FG5.1, 2, e
- KvK-nummer:5.1, 2, e
- Naam van het bedrijf of de organisatie
- Adres: Amstel 1
- Postcode: 1011PN Amsterdam
- Plaats: Amsterdam
- Hoofdsector: Openbaar bestuur
- Subsector: Gemeente

De rest van het formulier spreekt voor zich en bouwt zich stapsgewijs op. Het volledige AP-meldingsformulier wordt daarom niet beschreven in deze procedure.

2.7 Vraag FG om advies

Via 5.1, 2, i @amsterdam.nl kan de voorlopige melding worden meegestuurd richting de FG. Beschrijf wat er is gebeurd, en stuur het AP-meldingsnummer en rapport mee in de e-mail. Beschrijf ook expliciet of betrokkenen aldus de beoordeling van de Privacy Officer moeten worden geïnformeerd – en beargumenteer dit. In bepaalde gevallen is verplicht de AP je om betrokkenen te informeren, let daar dus extra op.

Let op; je bent zelf als Privacy Officer verantwoordelijk dat het datalek uiterlijk 4 weken na de vervolgmeldingdefinitief wordt gemaakt, zie ook 2.10 Maak AP melding definitief.

Betrokkene is degene wiens persoonsgegevens betrokken zijn bij het datalek. Een melding aan betrokkene is op grond van artikel 34 lid 1 AVG noodzakelijk als het datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van die persoon.

De lat ligt hier dus hoger dan bij een melding aan de AP, want het is enkel verplicht een melding te doen aan betrokkene als sprake is van en 'hoog risico'. Bij een hoog risico moet je denken aan situaties waarop de kans op bijv. discriminatie, identiteitsfraude, reputatieschade of financieel nadeel hoog is.

Het risico voor betrokkenen is al snel hoog als er bijzondere persoonsgegevens zijn betrokken bij het datalek. Als bijvoorbeeld een patiëntendossier van de GGD op straat komt te liggen, zijn er gezondheidsgegevens bij betrokken. Het gevolg van het datalek is onder andere dat er een schending is van bescherming van door het beroepsgeheim beschermde gegevens.

Een andere situatie waarbij je al snel te maken hebt met een hoog risico, is als identiteitskaarten zijn betrokken. Er is dan een risico op identiteitsfraude. Als er ook nog contactgegevens bij het datalek zijn betrokken, wordt het risico daarop alleen maar groter. Als gevolg van de identiteitsfraude kan betrokkene financieel nadeel lijden.

Soms wordt besloten om uit transparantieoverwegingen een melding te doen aan de betrokkene. Dit speelt bijvoorbeeld als iemand meldt dat een verklaring dat iemand een essentieel beroep uitoefent per abuis in zijn of haar personeelsdossier zit. Het is niet een gevoelig gegeven en het geeft geen hoog risico voor betrokkene. De medewerker kan op intranet worden opgezocht en dan is zijn of haar functie ook bekend. Het feit dat iemand in een essentieel beroep werkzaam is, lijkt niet tot enig nadeel te kunnen leiden voor betrokkene. Echter, het is wel zo transparant om richting een werknemer aan te geven dat deze verklaring bij iemand anders in het dossier zat.

2.8 Adviseert over AP en informeren betrokkenen

De FG zal adviseren over de datalekmelding. Zowel de keuze om de datalek (voorlopig) bij de AP te melden als het advies van de Privacy Officer w.b. het informeren van betrokkenen, wordt beoordeeld.

Het kan voorkomen dat de FG vragen heeft. Dan moet de Privacy Officer soms aanvullende informatie bij de melder of diens directie uitvragen. En de feedback van de FG meenemen in het verder afronden van de melding bij de AP.

Soms oordeelt de FG dat melden bij de AP niet nodig is - deze kan dan door de Privacy Officer worden ingetrokken.

2.9 Trek AP melding in

Wanneer de FG de melding bij de AP niet nodig vindt – of wanneer er anderzijds door nieuwe informatie geen sprake is van een hoog-risico datalek – kan de melding door de Privacy Officer worden ingetrokken. Dit kan via de website van de AP, met het voorlopige meldingsnummer. Overige maatregelen voor de directie met betrekking tot het datalek (*2.11 Maatregelen adviseren)* kunnen dan wel relevant blijven.

2.10 Maak AP melding definitief

Wanneer de FG zich kan vinden in de melding bij de AP, dient deze melding definitief te worden gemaakt wanneer alle informatie beschikbaar is. Dit wordt door de Privacy Officer gedaan. Een definitieve melding krijgt een nieuw meldingsnummer. Ook bevat deze niet alle informatie – alleen aangevulde informatie. Een volledig beeld van hetgeen gemeld is bij de AP wordt dus verkregen door voorlopige en definitieve meldingen *samen te voegen*.

Let op: een definitieve melding kan niet meer worden gewijzigd.

2.11 Maatregelen adviseren

Een herhaling van soortgelijke datalekken kan soms voorkomen worden – of de impact op betrokkenen kan worden verkleind. Datalekken kunnen worden voorkomen door bijvoorbeeld de beveiliging (AVG artikel 32) beter in te richten. De gevolgen voor betrokkenen kunnen worden gemitigeerd door bijvoorbeeld beter te kijken naar Privacy by Design of Privacy by Default (AVG artikel 25). Het nagaan van maatregelen bij het afronden van een onderzoek is daarom een essentiële stap in het datalekkenproces.

Het is belangrijk om – eventueel samen met de betreffende directie - het gesprek aan te gaan om soortgelijke datalekken te voorkomen of de impact daarvan te verkleinen.

2.12 Adviseert directie dringend betrokkenen te informeren, evt. maatregelen die betrokkenen zelf kunnen nemen

Wanneer de betrokkenen geïnformeerd dienen te worden over een datalek – en dit dus ook aan de AP is toegezegd - is het aan de Privacy Officer om dit te adviseren richting de melder en diens directie. Het is belangrijk om daarbij aan te geven dat het vanuit de AVG als wettelijk kader niet gaat om een advies om hen te informeren, maar een *verplichting*. Presenteer dit als een wettelijke bepaling die de directie verplicht om de betrokkenen te informeren. Verwijs hierbij naar de standaardbrief die voorhanden is om betrokkenen te informeren. Hoe deze brief eruit ziet, lees je in **Bijlage 2: Standaardbrief t.b.v het informeren van betrokkenen**. Is de directie niet voornemens om deze stap te zetten ongeacht dringend advies, zorg dan voor een passende escalatie.

In sommige gevallen zijn er maatregelen die *betrokkenen* kunnen nemen. Deze maatregelen worden tevens door de Privacy Officer opgesteld – maar zijn dus voor directe uitvoering van de betrokkene zelf. Denk bijvoorbeeld aan het advies tot wijzigen van een wachtwoord.

2.13 Informeert betrokkenen

De directie is zelf verantwoordelijk om betrokkenen te informeren. De standaardbrief in deze procedure is conform recente informatie (najaar '24) vanuit de AP herschreven. Los van tekstuele vereisten is het belangrijk dat:

- Deze stap zo snel mogelijk wordt gezet.
- De taal van het land van de slachtoffers wordt gehanteerd.

2.14 Treft geadviseerde maatregelen

De directie is zelf verantwoordelijk om maatregelen te nemen om datalekken te voorkomen – of de impact ervan te verkleinen.

2.15 Melding volledig maken, afmelden in TOPdesk

Aan het einde van de procedure maakt de Privacy Officer de TOPdesk melding compleet. Als deze volledig is ingevuld, kan deze worden afgesloten.

2.16 Ontvangt afmelding

Vaak wil de melder weten wanneer het onderzoek van de Privacy Officer is afgerond. Daarom is het aanbevolen om deze te informeren.

2.17 Ontvangt afmelding

De FG wil – indien er een definitieve melding bij de AP is gedaan – graag de afronding van het datalek ontvangen. Dat is dus een combinatie van de voorlopige *en* definitieve AP melding. Het is daarbij aanbevolen om ook de Privacy Officer van het betreffende organisatieonderdeel te betrekken – zeker als er mitigerende maatregelen zijn geadviseerd binnen de directie.

3. Bijlagen

Er zijn drie bijlagen relevant voor de datalekkenprocedure. Dit zijn:

- Bijlage 1: Handleiding TOPdesk
- Bijlage 2: Standaardbrief t.b.v het informeren van betrokkenen
- Bijlage 3: Veelvoorkomende datalekken (volgt in 2025)

Bijlage 1: Handleiding TOPdesk

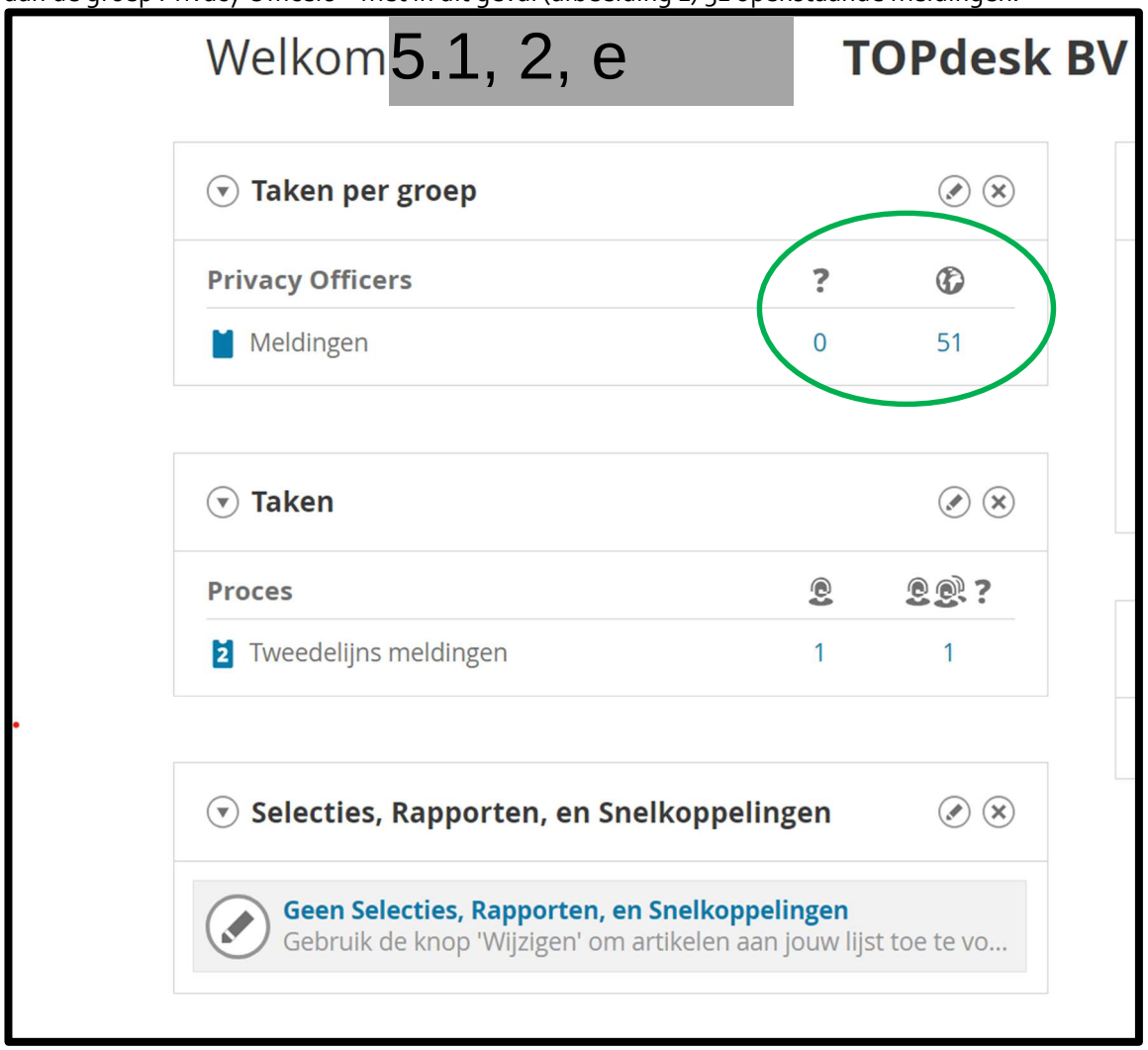
Inhoudsopgave

1. Startpagina, meldingen en zoeken
2. Nieuwe melding aanmaken (tab: Algemeen)
3. Beveiligingsincident invullen
- 3.1 Beveiligingsincident registreren
- 3.2 Beveiligingsincident als datalek samenvatten

4. Communiceren met de melder
5. TOPdesk standaardteksten instellen (eenmalig) en gebruiken
- 5.1 Standaardtekst toevoegen
- 5.2 Standaardtekst verdeling
- 5.3 De negen standaardteksten
  - 5.3.1 – Standaardtekst 1
  - 5.3.2 – Standaardtekst 2
  - 5.3.3 – Standaardtekst 3
  - 5.3.4 – Standaardtekst 4
  - 5.3.5 – Standaardtekst 5
  - 5.3.6 – Standaardtekst 6
  - 5.3.7 – Standaardtekst 7
  - 5.3.8 – Standaardtekst 8
  - 5.3.9 – Standaardtekst 9

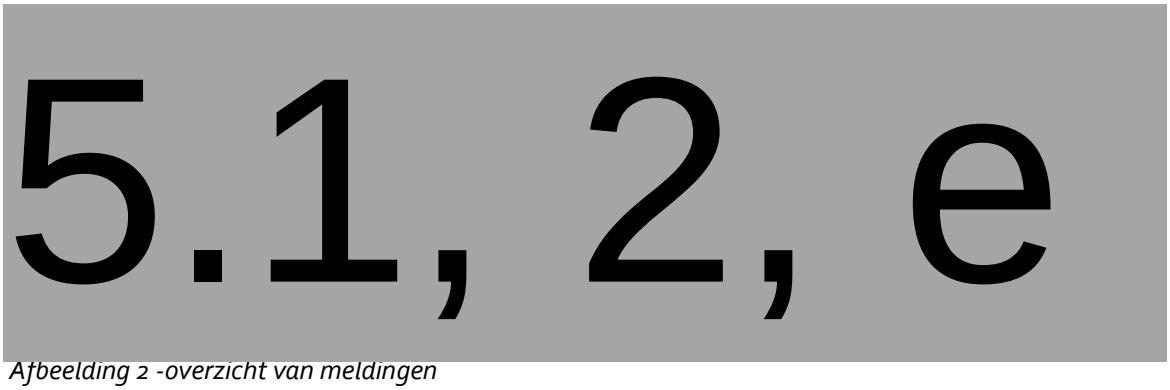
1. Startpagina, meldingen en zoeken

Nadat je bent ingelogd in TOPdesk, kom je op de startpagina. Hier zie je dat je bent toegevoegd aan de groep Privacy Officers – met in dit geval (afbeelding 1) 51 openstaande meldingen.



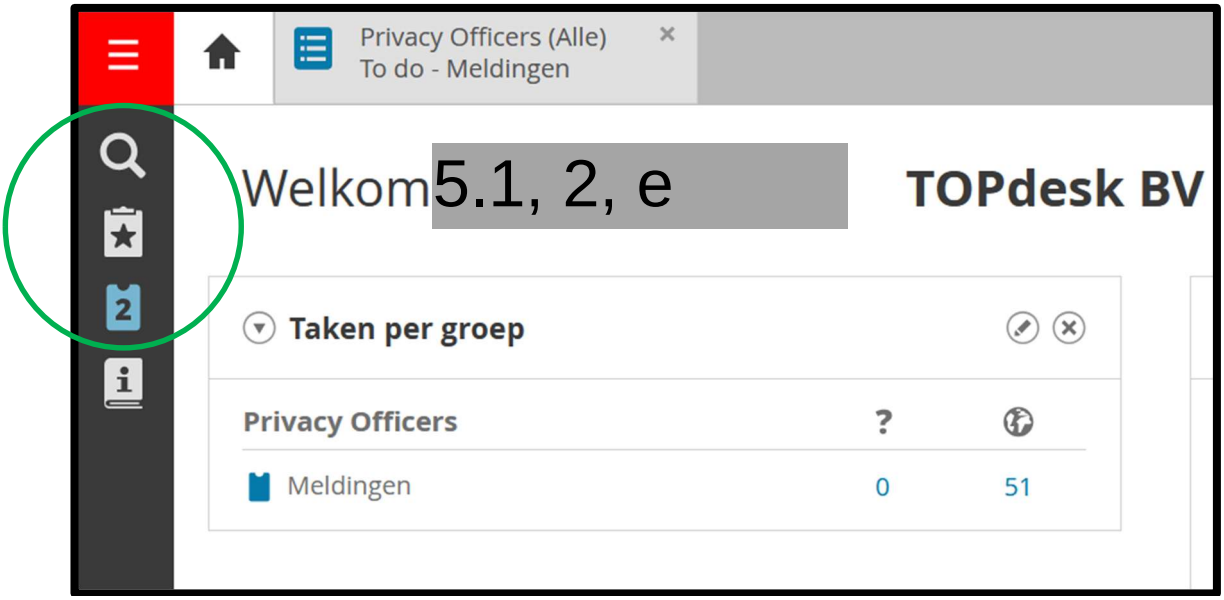
Afbeelding 1 -startpagina met 51-meldingen

Wanneer je op dit getal klikt, open je een lijst met al deze meldingen. In afbeelding 2 zie je daarnaast "FILTER: niet gereed" staan. Als je daarop klikt kan je je filter anders instellen – zo kan je andere lijsten met meldingen openen. Deze instellingen zijn gebonden aan jouw account – het is daarom belangrijk dat je een filter zo instelt dat je gemakkelijk kunt zien wanneer er nieuwe datalekmeldingen in TOPdesk zijn aangemeld.



Afbeelding 2 -overzicht van meldingen

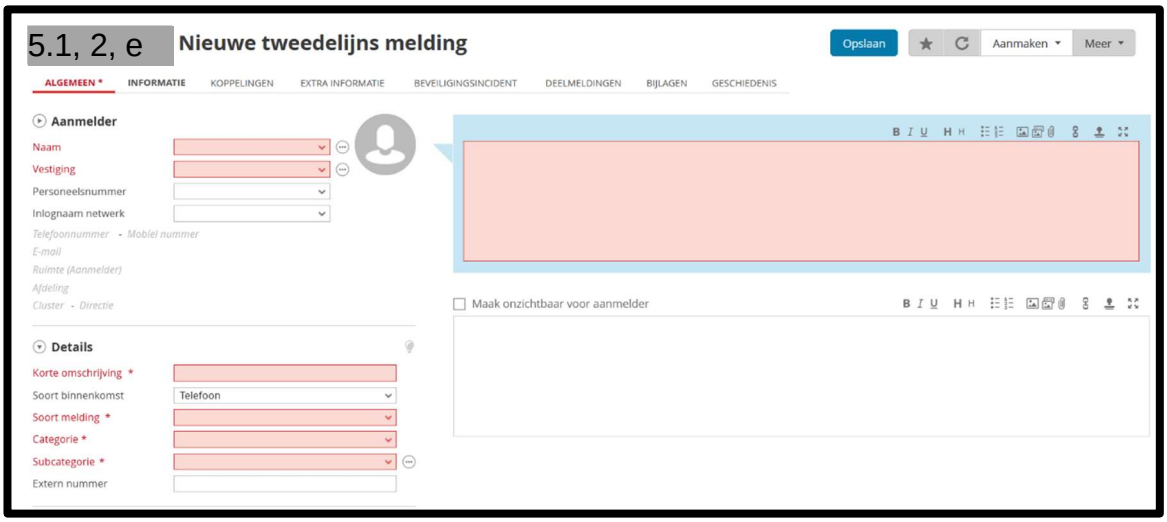
Soms wil je een bestaande TOPdesk melding opzoeken – dit kan via het vergrootglas in de linker kolom van TOPdesk. Daarnaast moet je soms zelf een melding aanmaken – het kan voorkomen dat meldingen wel via 5.1, 2, i @amsterdam.nl gemeld worden – maar deze nog niet in TOPdesk staan – of wel bestaan maar niet toegankelijk zijn voor de Privacy Officer vanwege rechten. De bestaande melding is dan al in behandeling bij collega's van Het Servicepunt. In dat geval moet je zelf een nieuwe tweedelijns melding aanmaken in TOPdesk. In het volgende hoofdstuk lees je hoe dit moet.



Afbeelding 3 – zoeken en nieuwe melding aanmaken

2. Nieuwe melding aanmaken (tab: Algemeen)

Nadat je een nieuwe melding hebt aangemaakt, opent onderstaand scherm. Je kunt in TOPdesk pas een melding maken en opslaan wanneer alle benodigde informatie is ingevuld. In dit hoofdstuk leggen we je uit wat je bij de velden moet invullen, in tab Algemeen.



Afbeelding 4 – een nieuwe, lege melding (deel 1)

Aanmelder
Typ de achternaam van de melder en selecteer de juiste persoon. De overige gegevens van de aanmelder worden dan vanzelf ingevuld. Controleer met overige informatie zoals e-mailadres of de juiste persoon is geselecteerd.

Verzoek
Dit is het roze grote invulveld, rechts. Vul hier de beschrijving van het datalek in. Vaak kun je de omschrijving uit een bestaande e-mail halen (bijvoorbeeld van Het Servicepunt).

Details

- Korte omschrijving: Beschrijf kort het datalek (bijv: kwijtgeraakte post of gestolen telefoon).
- Soort melding: kies Beveiligingsincident
- Categorie: kies Informatiebeveiliging
- Subcategorie: kies Datalek



Afbeelding 5 – een nieuwe, lege melding (deel 2)

Object/ruimte

- Betreft: kies Locatie
- Vestiging (Ruimte): typ N.v.t.
- Ruimte: typ n.v.t.

Planning

- Impact: in de meeste gevallen, na beoordeling hiervan, kun je kiezen voor "klein". Dit past de doorlooptijd en streefdatum ook aan. Mocht na beoordeling de impact groter blijken, dan kan dit worden aangepast naar "middel" of "groot". In beide gevallen is het goed om de melding te overleggen met iemand van de FG-office.
- Urgentie: ingeval van een kleine impact, "laag". Bij middel, "midden". Bij groot, "hoog".
- Prioriteit: ingeval van een kleine impact, kies voor "P4" of "P5". Bij middel, "P4" of "P3". Bij groot, "P2 of "P1".

Afhandeling

- Behandelaarsgroep: kies Privacy Officers
- Behandelaar: kies je eigen naam

Belangrijk: Sla nu je melding op (rechtsbovenaan, blauwe knop, Opslaan).

3. Beveiligingsincident invullen

Om het datalek goed te omschrijven, is het belangrijk om het tabblad Beveiligingsincident volledig in te vullen. Dit hoofdstuk beschrijft in 3.1 de drop-down menu's om het datalek te registreren. In 3.2 wordt beschreven hoe je een datalek samenvat. In 3.3 wordt beschreven hoe je TOPdesk standaardteksten kunt inrichten – dit is een eenmalige handeling.

3.1 Beveiligingsincident registreren

Klik op het tabblad Beveiligingsincident.



Afbeelding 6 – beveiligingsincident tabblad

Onderstaand tabblad wordt geopend.



Afbeelding 7 – beveiligingsincident invullen (deel 1)

Vul de velden in zoals hieronder omschreven. Elk kopje van het tabblad wordt apart toegelicht.

Classificatie IB incident

- IB Categorie: kies een optie die het meest van toepassing is
  Let op: Gaat het hier om een datalek onder de Wpg n.a.v. gelekte politiegegevens? Vul dan in: Inbreuk op politiegegevens
- IB Classificatie: hoef je niet in te vullen
- IB Soort: hoef je niet in te vullen

Omvang van het incident

- Cluster: kies het cluster waar het datalek is opgetreden
- Directie/stadsdeel: kies de directie/het stadsdeel waar het datalek is opgetreden
- Andere betrokken organisaties: geef aan als er een andere organisatie betrokken is bij het datalek

Datalek

- Datum/tijd constatering: Vul een datum en tijd in van de constatering van het datalek
- Gegrond: vink aan als het daadwerkelijk datalek betreft. *Let op: Is het geen datalek? Vink dan dit vinkje niet aan, omschrijf dit in de melding en sluit de melding af. De melding wordt dan niet geregistreerd als een datalek.*
- AP Classificatie: kies de meest passende categorie.

Datalek AP

*Let op: heb je bij de AP een melding gedaan? Zorg er dan voor dat als bijlage van de melding het PDF-rapport van de AP wordt toegevoegd. Vermeld ook in de omschrijving van de melding het meldingsnummer van de datalekmelding bij de AP. Doe dit bij voorlopige- **en** definitieve meldingen.*

- Melding AP?: Typ Ja, Nee of Voorlopig.
- Gemeld aan AP binnen 72 uur?: Typ Ja als binnen 72 uur een datalek is gemeld bij de AP. Typ Nee als dit niet is gedaan maar wel had gemoeten. Typ N.V.T. wanneer dit niet relevant is, omdat het datalek niet hoef te worden gemeld bij de AP.
- Datum/tijd melding bij AP: kies de juiste dag en tijd.



Afbeelding 8 – beveiligingsincident invullen (deel 2)

Groep Datalek – betrokkenen

- Betrokkenen geïnformeerd: Typ Ja of Nee.
- Datum/tijd melding aan betrokkenen: kies de juiste dag en tijd.

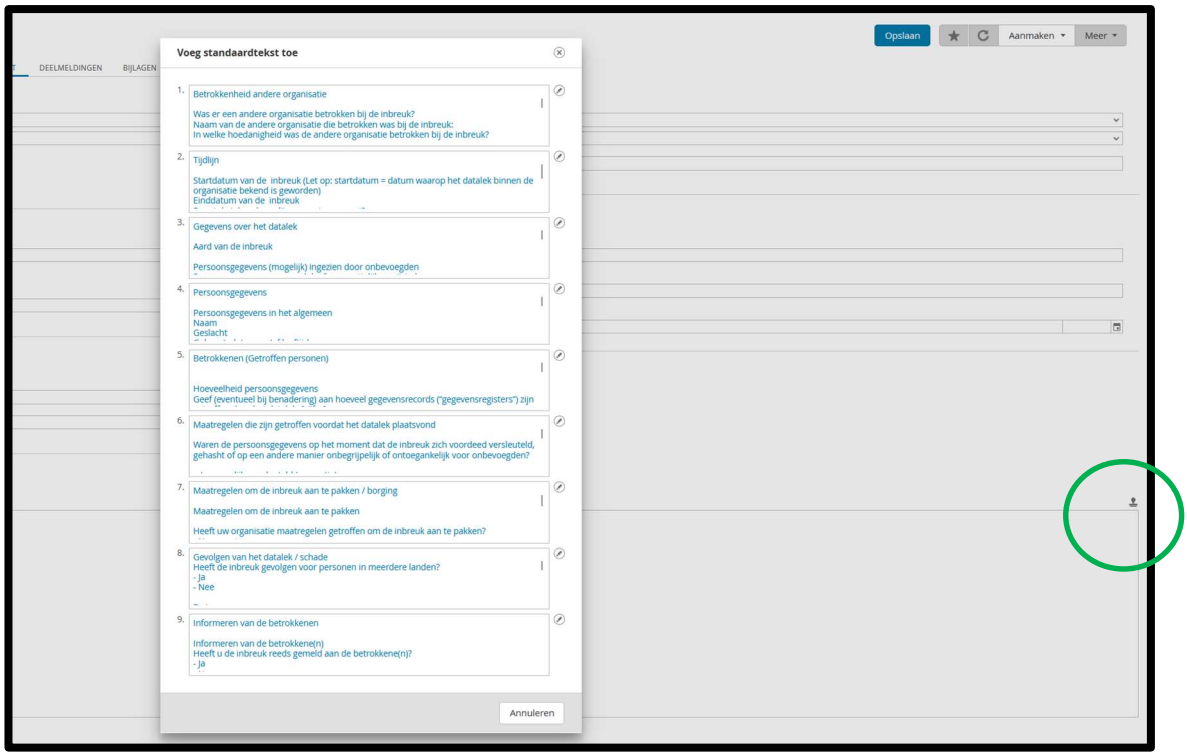
3.2 Beveiligingsincident als datalek samenvatten

Na het registreren van het datalek zijn er nog vijf memovelden die moeten worden ingevuld. Deze velden zorgen samen voor een goede samenvatting van het datalek. Het is belangrijk dat dit zo word ingevuld dat een collega – maar ook een AP als toezichthouder - begrijpt wat er is gebeurd en waarom keuzes zijn gemaakt die zijn gemaakt – bijvoorbeeld om een datalek niet bij de autoriteit persoonsgegevens te melden. Het betreft de velden:

- Omschrijving incident
- Borgende maatregelen
- Schade
- Toelichting 'Betrokkenen geïnformeerd'
- Toelichting 'Melding bij AP?'

Om aan de AVG verantwoordingsplicht te voldoen is het belangrijk om conform AVG artikel 33 (5) ook bij datalekken waar het risico voor betrokkenen onwaarschijnlijk is, dit datalek vast te leggen. De EDPB guidelines, specifiek richtlijn 121 t/m 125, beschrijven bijvoorbeeld essentieel is om te omschrijven waarom een toezichthouder *niet* op de hoogte is gebracht van een datalek. Om te zorgen voor een volledige verslaglegging van een datalek zijn in TOPdesk standaardteksten aanwezig. Deze teksten moeten eenmaal worden ingesteld (zie hoofdstuk 5) in een TOPdesk-account en kunnen daarna dienen als leidraad om het datalek volledig te omschrijven. De Privacy Officer is zelf verantwoordelijk om conform AVG en EDPB-guidelines een datalek van een volledige tijdlijn en samenvatting te voorzien – de standaardteksten kunnen daarbij helpen.

Klik op het icoontje en de standaardteksten worden geopend:

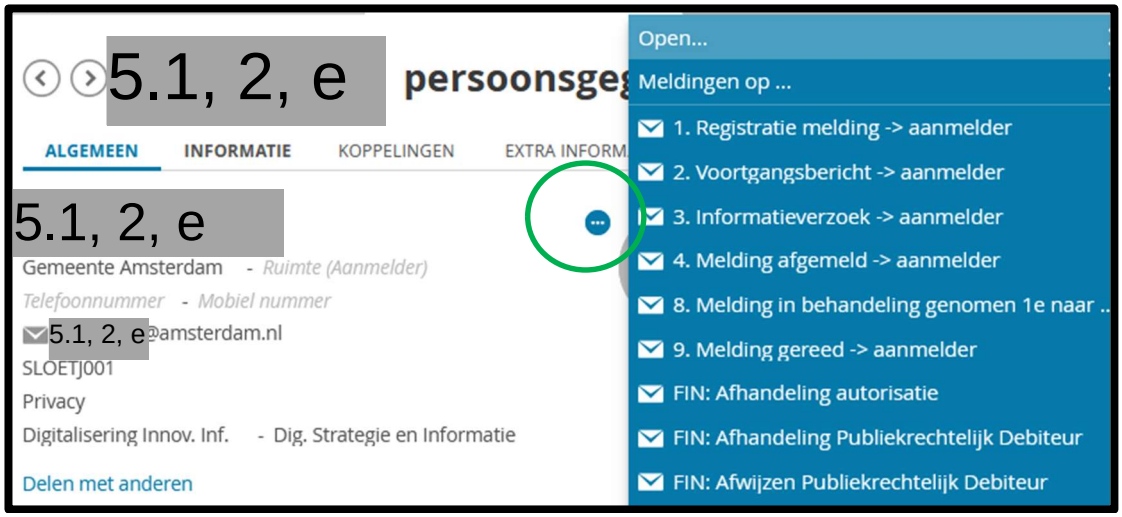


Afbeelding 9 – TOPdesk standaardteksten t.b.v. verantwoordingsplicht onder AVG. Komen tevoorschijn na het (kleine) knopje in rood omcirkeld

Belangrijk: Sla nu je melding op (rechtsbovenaan, blauwe knop, Opslaan).

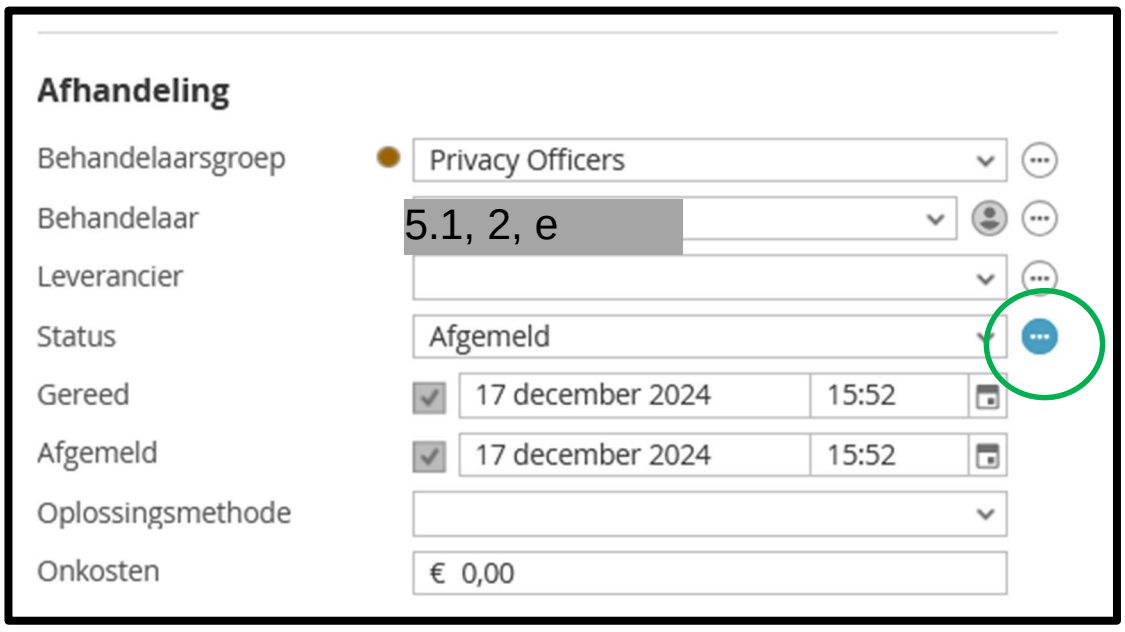
4. Communiceren met de melder

Soms is er informatie benodigd van de melder van het datalek. In TOPdesk zelf kun je gebruik maken van een e-mail template om de (aan)melder een bericht te sturen. Er zijn vele templates beschikbaar – deze zijn na keuze aanpasbaar. Tip: zorg ervoor dat de e-mail voor de melder begrijpelijk is en niet vol staat met onduidelijke of irrelevante informatie.



Afbeelding 10 – E-mail sturen naar aanmelder

Wanneer een melding is afgehandeld, is het aanbevolen de melder hiervan op de hoogte te brengen. Dat kan door middel van de knop, rechts van het menu *Status*.



Afbeelding 11 – Bericht sturen naar aanmelder dat melding is afgehandeld

5. TOPdesk standaardteksten instellen (eenmalig) en gebruiken

Zoals in hoofdstuk 3.2 beschreven, wordt aangeraden om TOPdesk standaardteksten te gebruiken om een datalek volledig samen te vatten. Dit hoofdstuk legt deze eenmalig worden ingesteld.

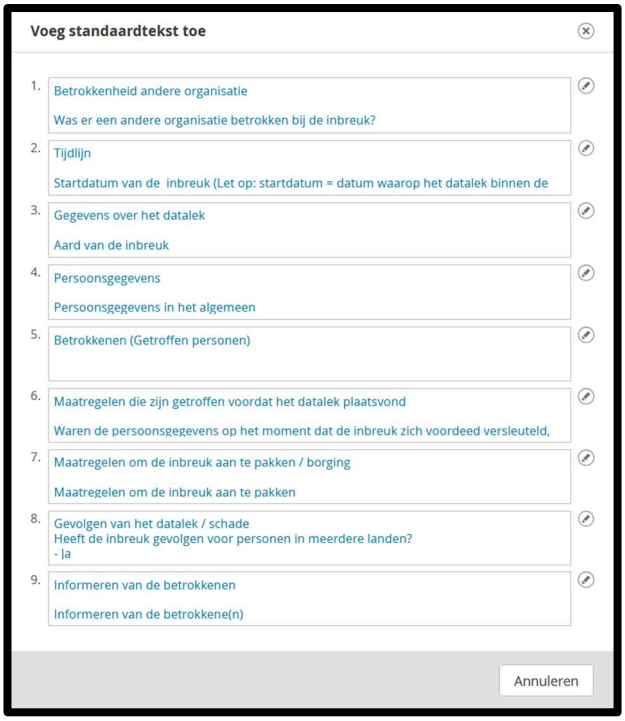
5.1 Standaardtekst toevoegen

Selecteer het tabblad Beveiligingsincident. Kies een memoveld, zoals Omschrijving incident. Klik op het knopje van Standaardtekst toevoegen.



Afbeelding 12 – Standaardtekst toevoegen

Er verschijnt een menu genaamd *Voeg standaardtekst* toe. In totaal zijn er negen velden met standaardteksten beschikbaar.



Afbeelding 13 – Reeds ingerichte standaardteksten

Initieel zijn deze velden allemaal leeg. In hoofdstuk 5.3 vind je alle standaardteksten die in deze negen velden geplakt moeten worden. Klik per veld op het pen-icoontje om deze tekst toe te voegen.

5.2 Standaardtekst verdeling

De standaardteksten kunnen worden ingezet voor de beschreven memovelden (zie hoofdstuk 3).
De negen standaardteksten zijn als volgt verdeeld per memoveld:

- Omschrijving incident - standaardtekst 1 tot en met 6
- Borgende maatregelen - standaardtekst 7
- Schade – standaardtekst 8
- Toelichting 'Betrokkenen geïnformeerd'- standaardtekst 9
- Toelichten 'Melden bij AP' – nog geen standaardtekst gedefinieerd

5.3 De negen standaardteksten

5.3.1 – Standaardtekst 1
Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?
Naam van de andere organisatie die betrokken was bij de inbreuk:
In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

Internationale aspecten

- Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?
- Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke EU-landen gaat het dan?
- Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?
- Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?

5.3.2 – Standaardtekst 2
Tijdlijn

Startdatum van de inbreuk (Let op: startdatum = datum waarop het datalek binnen de organisatie bekend is geworden)
Einddatum van de inbreuk
Duurt de inbreuk op dit moment nog voort?
Wanneer is het incident ontdekt?
Hoe is de inbreuk ontdekt?

Is er binnen de 72 uur gemeld aan de AP?
Zo nee, waarom niet?

5.3.3 – Standaardtekst 3

Gegevens over het datalek

Aard van de inbreuk

Persoonsgegevens (mogelijk) ingezien door onbevoegden
Persoonsgegevens per ongeluk of onopzettelijk gewijzigd
Persoonsgegevens permanent niet beschikbaar (verloren/verwijderd)
Persoonsgegevens tijdelijk niet beschikbaar

Aard van het incident
Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest? Kies 1 van de volgende opties:

a. Apparaat, gegevensdrager (bv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen
b. Autorisatie(s) van medewerker(s) verkeerd ingesteld
c. Brief of postpakket met persoonsgegevens geopend retour ontvangen
d. Brief of postpakket met persoonsgegevens kwijtgeraakt
e. Brief of postpakket met persoonsgegevens verstuurd of afgegeven aan de verkeerde ontvanger(s)
f. E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)
   - Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?
     i. Ja
     ii. Nee
     iii. De verkeerde ontvanger heeft niet gereageerd
g. E-mail verstuurd met persoonsgegevens met ontvangers in het aan-veld of in de cc, in plaats van bcc
h. Phising
i. Ransomware
j. Ander type hacking en/of malware
k. Netwerkmappen of –locaties met persoonsgegevens zijn te breed toegankelijk ingesteld binnen de organisatie
l. Overig, namelijk:
m. Persoonsgegevens bij oud papier gezet
n. Persoonsgegevens door storing (tijdelijk) niet beschikbaar
o. Persoonsgegevens per ongeluk gepubliceerd
p. Persoonsgegevens toegevoegd aan het verkeerde dossier
q. Persoonsgegevens van verkeerde klant getoond in klantportaal

Samenvatting datalek: (beschrijving van het incident)

5.3.4 – Standaardtekst 4
Persoonsgegevens

Persoonsgegevens in het algemeen
Naam
Geslacht
Geboortedatum en/of leeftijd
Burgerservicenummer (BSN)
Contactgegevens, geef aan welke:
- Adres en woonplaats
- E-mailadres
- Telefoonnummer

Toegangs- of identificatiegegevens (bijvoorbeeld gebruikersnamen en wachtwoorden

Financiële gegevens, geef aan welke:
- IBAN
- Creditcardgegevens
- Gegevens over (problematische) schulden
- Gegevens over uitkering en/of toeslagen
- Andere financiële gegevens

(Kopieën van) paspoorten of andere legitimatiebewijzen
Locatiegegevens

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

Anders, namelijk:
Onbekend

Bijzondere persoonsgegevens
Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
Persoonsgegevens waaruit iemands politieke opvattingen blijken
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Gegevens over iemands gezondheid
Genetische gegevens
Biometrische gegevens (bijv. vingerafdruk of irisscan)

5.3.5 – Standaardtekst 5
Betrokkenen (Getroffen personen)

Hoeveelheid persoonsgegevens
Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door het datalek: [cijfer]

Is het exacte aantal betrokkenen bekend?
Zo ja → het exacte aantal is: [cijfer]
Zo nee:
- het minimum aantal betrokkenen is:
- het maximum aantal betrokkenen is:

Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk:

Type betrokkenen (personen van wie persoonsgegevens zijn getroffen door de inbreuk):
Werknemers
Klanten (huidig en potentieel)
Leerlingen of studenten
Patiënten
Minderjarigen
Personen uit kwetsbare groepen
Anders, namelijk:

Geef een nadere omschrijving van de groep(en) betrokkenen (dus van de mensen van wie persoonsgegevens zijn betrokken bij de inbreuk):

5.3.6 – Standaardtekst 6

Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?

- Ja, namelijk: versleuteld (encryptie)

Geef aan : welke versleutelingstechniek heeft u toegepast (indien bekend)?
Probeer waar mogelijk ook details te geven, zoals het aantal bits van de gebruikte sleutel en de standaard (bijv. AES-256). Let op: indien een laptop of andere drager beveiligd is met een wachtwoord betekent dat niet altijd dat de gegevens op de drager zijn versleuteld en onder 'versleuteld' wordt niet bedoeld: versleuteld door een ransomware aanval.

- Ja, namelijk gehasht

Geef aan: welke hashingtechniek heeft u toegepast (indien bekend)?
Bijv. MD5, SHA-256, of een andere cryptografische hashfunctie. Geef hierbij ook aan of gebruik is gemaakt van een salt.

- Ja, namelijk: op een andere manier onbegrijpelijk of ontoegankelijk gemaakt

Bijv. standaard versleutelde soft- of hardware of andere beveiligingsmethoden.

- Nee

5.3.7 – Standaardtekst 7

Maatregelen om de inbreuk aan te pakken / borging

Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

- Nee, want :
- Nog niet bekend
- Ja, namelijk :
-

Heeft uw organisatie maatregelen getroffen om **nieuwe** soortgelijke inbreuken te voorkomen?

- Nee, want:
- Nog niet bekend
- Ja, namelijk:

5.3.8 – Standaardtekst 8

Gevolgen van het datalek / schade

Heeft de inbreuk gevolgen voor personen in meerdere landen?

- Ja
- Nee

Zo ja:

- Bevindt de hoofdvestiging of de enige vestiging van uw organisatie zich in Nederland?
  - Ja
  - Nee
- Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke landen gaat het dan?

(Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens

- Onbevoegden hebben kennis kunnen nemen van de gegevens
- De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt
- Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt
- Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties
- Een essentiële dienst kan tijdelijk niet meer worden verleend aan degenen van wie gegevens zijn gelekt (de betrokkenen)
- Een essentiële dienst kan permanent niet meer worden verleend aan degenen van wie gegevens zijn gelekt (de betrokkenen)
- Anders, namelijk:

(Mogelijke) gevolgen voor de betrokkene(n)
Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

- Discriminatie of uitsluiting
- Identiteitsdiefstal of -fraude
- Financieel verlies
- Reputatieschade
- Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
- Ongeoorloofde ongedaanmaking van pseudonimisering
- Betrokkenen kunnen bijvoorbeeld (de verwerking van) hun persoonsgegevens niet inzien of op verzoek laten verwijderen (Uitoefening rechten)
- Betrokkenen verliezen het overzicht van welke organisaties hun persoonsgegevens verwerken en worden verhinderd controle uit te oefenen

Anders, namelijk: [invullen]

Inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen:

- Verwaarloosbaar
- Beperkt
- Aanzienlijk
- Zeer groot

Toelichting:

5.3.9 – Standaardtekst 9

Informeren van de betrokkenen

Informeren van de betrokkene(n)
Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?

- Ja
- Nee

Zo ja:

- Aan hoeveel personen wilt u de inbreuk gaan melden?
- Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?
- Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?
- Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Zo nee:

- Gaat u de inbreuk nog melden aan betrokkene(n)?
    - Ja:
        - Aan hoeveel personen gaat u de inbreuk melden?
        - Wanneer gaat u (naar verwachting) de inbreuk melden aan betrokkene(n)?
        - Licht toe aan welke (groep) betrokkene(n) u de inbreuk gaat melden
    - Nee:
        - Motivering niet (persoonlijk) informeren van de betrokkene(n)
            - Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?
                - Het zou een onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren + LICHT TOE waarom het een onevenredige inspanning zou vergen om iedere betrokkene op individuele basis te informeren
                - De maatregelen die ik heb getroffen voordat de inbreuk plaatsvond bieden voldoende bescherming om de melding aan betrokkene achterwege te kunnen laten + GEEF AAN WELKE MAATREGELEN u heeft getroffen waardoor het niet nodig is om de betrokkene te informeren
                - Ik heb na de inbreuk maatregelen genomen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico zal voordoen voor de rechten en vrijheden van betrokkenen + GEEF AAN WELKE MAATREGELEN u heeft getroffen waardoor het niet nodig is om betrokkenen te informeren.
                - Andere reden(en), namelijk: [INVULLEN]
                - Er is sprake van een zwaarwegend belang om de getroffen personen niet te informeren, namelijk: [INVULLEN]
                  Getroffen personen hoeven niet te worden geïnformeerd als dat noodzakelijk en evenredig is ter bescherming van:
                    - De nationale veiligheid
                    - Landsverdediging
                    - De openbare veiligheid
                    - De voorkoming het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid
                - Andere belangrijke doelstellingen van algemeen belang van de EU of van Nederland ,met name een belangrijk economisch of financieel belang van de EU of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid, en sociale zekerheid
                - De bescherming van onafhankelijkheid van de rechter en gerechtelijke procedures
                - De voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen
                - Een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, als is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d en g van artikel 41 lid 1 UAVG
                - De bescherming van de betrokkene of van de rechten en vrijheden van anderen of de inning van civielrechtelijke vorderingen.
    - Nog niet bekend:
        - LET OP: je moet er vanuit gaan dat de inbreuk aan betrokkene(n) **moet** melden
        - Als het gaat om:
            - Bijzondere persoonsgegevens
            - Strafrechtelijke persoonsgegevens
            - Persoonsgegevens van mensen uit een kwetsbare groep

        - Veel persoonsgegevens of van persoonsgegevens van veel betrokkenen
    - En/of de inbreuk kan leiden tot:
        - Discriminatie of uitsluiting
        - Identiteitsfraude of –diefstal
        - Financiele verliezen
        - Reputatieschade
        - Doorbreking van beroepsgeheim

Zie ook: 'Guidelines meldplicht datalekken' van de AP.

Bijlage 2: Standaardbrief t.b.v het informeren van betrokkenen

In deze bijlage zijn twee standaardbrieven opgenomen. De bedoeling is dat in de vastgestelde procedure één standaardbrief wordt opgenomen die voldoet aan de AVG en specifiek de richtlijnen van najaar '24 over hoe betrokkenen van een datalek worden geinformeerd.

- Brief 2a is recent opgesteld door een collega Privacy Officer n.a.v. deze richtlijnen.
- Brief 2b is ouder format (2023), vermoedelijk vaker gebruikt in de vakgroep.

Om aan de richtlijnen van de AP te voldoen, is nog een verbeterslag nodig. Specifiek doel ik dan op:

- Inkorten van zinnen en versimpelen van jargon
- Tussenkoppen toevoegen
- Lange opsommingen inkorten
- Optie: paragraaf die aangeeft dat een brief nog opvolging krijgt als meer informatie bekend is over het datalek
- Specifieker omschrijven wat waarschijnlijke gevolgen zijn voor slachtoffers

Een deel van deze verbeterpunten kan evt. door communicatie worden gedaan – zeker wat betreft de leesbaarheid. Daarom is het belangrijk dat er vanuit de vakgroep een verbeterslag plaatsvindt op een standaardbrief waarna deze door communicatie, met inachtneming van de richtlijnen van de AP conform leesbaarheid zoals zinslengte, wordt vastgesteld en in deze procedure wordt opgenomen.

Bijlage 2a. Standaardbrief betrokkene (opgesteld dec '24)

Onderzoek en Statistiek

Postbus 23475

1100 DZ Amsterdam

020 255 4800

amsterdam.nl

5.1, 2, e

Retouradres: Postbus 23475, 1100 DZ Amsterdam

Datum	10 december 2024
Kenmerk	S-/
Onderwerp	Mededeling van een data-lek

Geachte meneer/mevrouw [persoon],

Hierbij willen wij u informeren over een geconstateerd datalek die uw persoonsgegevens heeft geraakt.
U heeft zich aangemeld als panellid om vragenlijsten in te vullen. Daarvoor heeft u toegang tot een panelomgeving. Er is vastgesteld dat uw inloggegevens voor deze panelomgeving van de Gemeente Amsterdam door een kwaadwillende zijn gestolen en dat deze online te koop worden aangeboden. Deze inloggegevens bestaan uit uw emailadres en het door u gekozen wachtwoord. Op dit moment kan er niemand meer in uw panelomgeving door maatregelen die we voor u hebben genomen, maar het is mogelijk dat er in het verleden wel kwaadwillenden zijn geweest die op uw account hebben ingelogd.
Als iemand inderdaad met deze gegevens heeft ingelogd op de panelomgeving zou deze persoon de door u ingevulde data kunnen inzien, dit zijn mogelijk onder andere uw: voornaam, tussenvoegsel, achternaam, postcode, geslacht, geboortedatum, aantal personen in het huishouden, samenstelling huishouden, eventueel aantal kinderen jonger dan 18 jaar en ouder dan 18 jaar, inkomenscategorie, hoogst voltooide opleiding, geboorteland panellid en geboorteland ouders. Als u deze gegevens niet zelf heeft ingevuld in de panelomgeving, dan kunnen onbevoegden deze gegevens ook niet hebben kunnen inzien.
Gemeente Amsterdam houdt goed in de gaten of er gegevens van mensen, die betrokken zijn bij de gemeente, online worden aangeboden en de gemeente heeft dus onderzoek gedaan zodra werd gezien dat uw gegevens online werden aangeboden. Uit dit onderzoek blijkt dat er waarschijnlijk op uw eigen computer/tablet/etc. malware is geïnstalleerd waardoor uw inloggegevens van uw eigen apparaat zijn gestolen. Dit kan bijvoorbeeld

gebeuren als er op een malafide link wordt geklikt. De exacte manier waarop dit op uw apparaat is gebeurd kunnen wij vanuit de gemeente niet zien.
Daarop heeft de gemeente alvast de volgende acties voor u ondernomen:

- Uw wachtwoord voor de panelomgeving van de gemeente is gereset zodat onbevoegden niet meer gebruik kunnen maken van de online aangeboden inloggegevens;
- Er is een datalekmelding voor u gemaakt bij de AP;
- We hebben u, wiens gegevens online te koop zijn aangeboden, hierover geïnformeerd.

Wij willen u graag ondersteunen bij veilig internetgebruik. In een wereld waar digitale dreigingen steeds vaker voorkomen, is het namelijk van groot belang om bewust en zorgvuldig om te gaan met persoonlijke gegevens en apparaten.
Daarnaast hebben wij nog enkele concrete tips voor u:

1. Wijzig uw wachtwoord op de panelomgeving van de gemeente, dat doet u door bij het inloggen te klikken op 'wachtwoord vergeten';
2. Als u dit wachtwoord ook voor andere accounts buiten de gemeente gebruikt raden wij u dringend aan deze allemaal wijzigen;
3. Zorg ervoor dat u voor al uw verschillende accounts allemaal verschillende wachtwoorden gebruikt;
4. Installeer, waar mogelijk, bij al uw accounts multi factor authenticatie (MFA) zodat u bijvoorbeeld een sms of email krijgt als iemand probeert in te loggen op uw account. Dit is ook vanaf januari 2025 mogelijk in de panelomgeving van de gemeente;
5. Schaf een goede virusscanner aan voor uw computer als u dit nog niet heeft gedaan, de consumentenbond heeft enkele virusscanners met elkaar vergeleken: Beste virusscanner 2024 | Consumentenbond;
6. U kunt overwegen om bij de politie aangifte te doen tegen de kwaadwillenden die de malware op uw computer hebben gezet en zo uw inloggegevens van u hebben gestolen.

Voor uitgebreide informatie en praktische tips nodigen wij u tot slot uit om de volgende betrouwbare websites te bezoeken:

- Politie.nl: Informatie over het herkennen van gehackte accounts en de stappen die u kunt ondernemen: Er staat mogelijk malware op mijn computer. Wat moet ik doen? | politie.nl
- Veilig Internetten: Hier vindt u basisveiligheid en handige stappen om uw online aanwezigheid beter te beschermen: Antwoord op vragen en hulp bij problemen. Voor iedereen.
- Digital Trust Center: Richtlijnen en ondersteuning bij het herstellen van gehackte accounts: Home | Digital Trust Center (Min. van EZ)

Deze bronnen bieden duidelijke en toegankelijke informatie om u te helpen de controle over uw digitale veiligheid te behouden. We raden u aan om regelmatig deze bronnen te raadplegen en u bewust te blijven van de laatste adviezen op het gebied van online veiligheid.

Wij betreuren ten zeerste dat uw gegevens online worden aangeboden en hebben passende maatregelen genomen om u te ondersteunen in uw digitale veiligheid. Helaas is het niet mogelijk om uw inloggegevens van het internet te halen omdat niet te achterhalen is wie achter de verkoop ervan zit. Met bovenstaande stappen kunt u er wel voor zorgen dat de aangeboden gegevens niets meer waard worden (want de inlogpoging zal niet succesvol zijn) en de ervaring leert dat de gegevens er dan snel worden afgehaald.

Wilt u meer informatie of heeft u vragen, dan kunt u contact op nemen met [persoon]. Hij/Zij is bereikbaar op telefoonnummer [*nummer*] of per e-mail: [...]@amsterdam.nl.

Met vriendelijke groet,

Namens directie Onderzoek en Statistiek van de Gemeente Amsterdam,
[persoon]

Bijlage 2b. Standaardbrief betrokkene (opgesteld '23)

Belastingen

Gemeente Amsterdam

Postbus 23475

1100 DZ Amsterdam

020 255 4800

amsterdam.nl

Retouradres: Postbus 23475, 1100 DZ Amsterdam

Datum 14 april 2023
Kenmerk S-/
Onderwerp Mededeling van een datalek

Geachte meneer/mevrouw,

Hierbij willen wij u informeren over een geconstateerd datalek bij Gemeente Amsterdam die (mogelijk) uw persoonsgegevens heeft geraakt.

Onlangs is vastgesteld dat een kopie van uw gecombineerde aanslag 2023 met uw persoonsgegevens (uw naam, uw adres en de hoogte van de opgelegde gecombineerde aanslag) per abuis per e-mail is verstuurd aan een ander persoon met identieke naam. Dit is het gevolg van foutief menselijk handelen.

De volgende acties hebben wij ondernomen om dit handelen te herstellen:

1. De medewerkers die bij deze handelingen zijn betrokken zijn hierover geïnformeerd;
2. Er zal op onze afdeling aandacht worden gevraagd om meer oplettendheid bij het versturen van gegevens;
3. Er is een datalek-melding gemaakt bij het servicepunt van Gemeente Amsterdam;
4. Er is telefonisch contact opgenomen met de persoon die uw gegevens heeft ontvangen. Deze persoon is verzocht om de mail met uw gegevens te verwijderen. Dit is inmiddels door deze persoon gedaan en is schriftelijk aan ons bevestigd.

Wij hechten er veel waarde aan dat u erop kunt vertrouwen dat uw persoonsgegevens binnen onze organisatie in goede handen zijn. Wij doen er veel aan om uw persoonsgegevens te beveiligen en zetten alle redelijke middelen in die technisch en organisatorisch mogelijk zijn om dit te bewerkstelligen.

Wij bieden u onze excuses aan en betreuren ten zeerste dat uw gegevens tijdelijk bij een ander persoon terecht zijn gekomen. Wij hebben door het nemen van de bovenstaande acties beoogd dat een verdere verspreiding van of toegang tot uw persoonsgegevens beperkt is. U hoeft zelf geen nadere maatregelen te nemen.

Wilt u meer informatie of heeft u vragen, dan kunt u contact op nemen met [*naam medewerker*]. *Hij/zij* is bereikbaar op telefoonnummer [*nummer*] of per e-mail: [...]@amsterdam.nl. **Vragen**
Hebt u vragen? Kijk dan op amsterdam.nl/belastingen. Of bel ons op 020 255 4800. Wij zijn bereikbaar van maandag tot en met vrijdag van 08.00 uur tot 18.00 uur. Voor een bezoek aan een van de Stadsloketten kunt u via dit nummer een afspraak maken. U vindt documenten zoals aanslagen, bezwaaruitspraken, etc. op mijnbelastingen.amsterdam.nl (inloggen met DigiD of eHerkenning).

Met vriendelijke groet,

[Naam]
[Functie]
Gemeente Amsterdam

Bijlage 3: Analyse van veelvoorkomende datalekken (volgt in 2025)

Ten behoeve van uniformiteit in de afhandeling van datalekken, en op verzoek van de FG, zal in een latere versie deze bijlage worden toegevoegd. Er is in het verleden vanuit de vakgroep documentatie hierover opgesteld, die kan als basis dienen voor deze bijlage.